PayPal Online Card Payment Services Agreement

Print

Last Update: May 6, 2022

This PayPal Online Card Payment Services Agreement ("Agreement") contains the terms of a contract between you (also referred to as the “Merchant”) and PayPal (Europe) S.àr.l. et Cie, S.C.A. ("PayPal" or "we").

PayPal is licensed as a Luxembourg credit institution and is under the prudential supervision of the Luxembourg supervisory authority, the Commission de Surveillance du Secteur Financier (the "CSSF"). The CSSF has its registered office in L-1150 Luxembourg.

About this Agreement

This Agreement applies to you if you are registered with PayPal as resident of Austria.

By integrating or using any of the Products or Online Card Payment Services you agree to be bound by the terms of this Agreement. If you are offered and choose to use any Product, Online Card Payment Service or functionality (including technology) mentioned in this Agreement, the terms in this Agreement relating to that Product, Online Card Payment Service or functionality apply.

The Products are:

- **Website Payments Pro** - a suite of functionality consisting of Express Checkout, Direct Payments API, Virtual Terminal and Fraud Management Filters as standard. Optional additional services include Fraud Protection, Advanced Fraud Management Filters and the Recurring Payments Tool;
- **Advanced Credit and Debit Card Payments** - a suite of functionality consisting of Advanced Credit and Debit Card Payments API as standard and Fraud Protection as an optional additional service. We may also offer you as optional additional services any of the following:
    - any Website Payments Pro functionality,

    - the Vaulting Tool, and
    - the Account Updater Service.
- Virtual Terminal – the Virtual Terminal functionality as a standalone Product.

Each of the Products includes one or more Online Card Payment Services. The Online Card Payment Services are:

- **Direct Payments API** - Functionality for performing credit and debit card transactions, where the card details are entered online by the cardholder.
- **Advanced Credit and Debit Card Payments API -** Functionality for performing credit and debit card transactions, where the card details are entered online by the cardholder, as an alternative to the Direct Payments API.
- **Virtual Terminal** - Functionality provided by PayPal to enable you to receive a card payment by manually entering Card Data given to you by the cardholder.

The User Agreement for PayPal Service (which we call here the **User Agreement**), Commercial Entity Agreement and Privacy Statement form part of this Agreement. See section 5 for more provisions relating to how these other legal documents apply.

We may amend, delete or add to this Agreement in line with the Change process set out in the User Agreement. If you do not agree with any Change, you may terminate this Agreement as set out in section 8 of this Agreement.

Please view **download and save** this agreement.

1. Setting up and activating your Product

1.1. Getting started

To obtain and use your Product, you must first do all of the following:

1.1.1. Complete the online application and approval process for your Product, open a PayPal Business Account (if you do not already have one), and follow the instructions set out in PayPal's online process to access and use your Product.

1.1.2. Integrate your Product into the payment process of your website, if your Product is Website Payments Pro or Advanced Credit and Debit Card Payments. You are not required to integrate your Product into the payment process of your website if you only access and use Virtual Terminal. PayPal is not responsible for any problems that could occur by integrating your Product into your 'live' website.

1.1.3. Activate your Product by using it in a 'live' payment transaction for the first time.

If your Product is Website Payments Pro or Advanced Credit and Debit Card Payments, we may allow you to integrate and use the Direct Payments API or Advanced Credit and Debit Card Payments API– as a PayPal Hosted Integration or Self Hosted Integration.

We may set either Hosting Option as your default option for integrating the Direct Payments API or Advanced Credit and Debit Card Payments API into the payment process of your website.

1.2. Required use of Express Checkout

If we offer you Express Checkout functionality as part of your Product and you choose to use that Product, you must implement PayPal Express Checkout as part of your website integration. In implementing Express Checkout, you agree that your website:

1.2.1. Includes a PayPal Express Checkout button either: (A) before you request the shipping/billing address and other financial information from your customers or (B) on the same page that you collect such information if you only use one page for your checkout process.

1.2.2. Offers PayPal as a payment option together with the other payment options you offer for Express Checkout. The PayPal logo must be displayed with equal or greater prominence as the logos for your other payment options.

1.2.3. Provides your customers with the option of not storing their personal information, including their email address, shipping/billing address, and financial information, as part of the checkout process.

1.3. Cancellation

We may terminate your access to and/or use of any or all Products and / or terminate this Agreement at any time before the Activation Date by notifying you.

2. Fees

2.1 How fees are paid

You agree to pay the fees in this Agreement as they become due without set-off or deduction. You authorise us to deduct our Fees from the amounts we transfer but before those funds are credited to your Account.

Except as further provided in this Agreement, you agree to pay the fees set out in the User Agreement.

Fees will be charged in the currency of the payment received.

2.2. Transaction Fees for Standard PayPal Payments

The Fees for receiving Domestic Transactions (Selling) as outlined in the User Agreement to applies to each domestic Standard PayPal Payment you receive.

2.3 Transaction Fees for Receiving Card Payments

The fees called out in the User Agreement for receiving payments in your PayPal account apply to each payment you receive from a card using the Online Card Payment Services. If you opt to be charged under the Interchange Plus Fee Structure, you will be charged the fees called out in the User Agreement for receiving payments in your PayPal account plus the Interchange Fee.

2.4. Additional Transaction Fees

The fee for Receiving Cross Border payments (Selling) applies as outlined in the User Agreement, except that it does not apply to payments received from cards using the Online Card Payment Services under the Interchange Plus Fee Structure.

2.5. Monthly Reports on Transaction Costs

PayPal shall make available monthly reports on transaction costs (inclusive of interchange fees) for card transactions which you process with the Product. These reports will be downloadable from your PayPal account. The reports do not include any Standard PayPal Payments.

3. Choice of Interchange Plus Fee Structure and Blended Pricing Fee Structure

You may choose the fee structure applicable to you for your receipt of card payments through any of the Online Card Payment Services (including via Direct Payment API, Advanced Credit and Debit Card Payments API and/or Virtual Terminal) by the methods or procedures that PayPal may make available to you. If you do not make an election, you will stay on your existing fee structure.

You may choose your fee structure for future transactions only, not for past transactions. This means that if you opt to be charged under the Interchange Plus Fee Structure, the respective Interchange Plus Fee Structure will apply to the use of both our Online Card Payment Services and PayPal Here.

Interchange Fees are set by Visa and MasterCard. They vary for different types of cards (for example by categories and brand). **PayPal shall always charge you the Interchange Fee as set by Visa and MasterCard and as passed on by its Acquirer.**

Single Interchange Fees may change from time to time. For more information on Interchange Fees, please see **MasterCard's** and **Visa's** website as well as our **simplified overview**.

If you opt to be charged under the Interchange Plus Fee Structure you agree that when PayPal receives a card payment for you through any of the Online Card Payment Services, PayPal may hold those funds in the Reserve Account portion of your PayPal Account before they reach the Payment Account portion of your PayPal Account. You instruct PayPal to pay those funds to your Payment Account only on the Business Day on which PayPal receives the information about the interchange fee applicable to the card payment. While the funds are held in your Reserve Account, the transaction will appear to you as "Pending" in your Account details. PayPal does not consider that the proceeds of the card payment in your Reserve Account are at your disposal until PayPal has received the information on the applicable interchange fee from our Processor (which can be within the next Business Day following the day on which the card payment was initiated by the card holder).

4. Information security; Data Protection; Data Portability

4.1. Compliance with Data Security Schedule

You agree (as a "Merchant") to comply with Schedule 1 below, which forms part of this Agreement.

4.2. Your PCI DSS compliance

You also agree to comply with the PCI Data Security Standard (PCI DSS). You must protect all Card Data that comes within your control according to PCI DSS, and you must design, maintain and operate your website and other systems in conformity with PCI DSS. You must ensure that your staff are and remain sufficiently trained so that they are aware of PCI DSS and can carry out its requirements. PayPal is not responsible for any costs that you incur in complying with PCI DSS. Find more information about PCI DSS at the PCI Security Standards Council's website here: **https://www.pcisecuritystandards.org/pci_security/**.

4.3. PayPal's PCI DSS compliance

PayPal warrants that PayPal and your Product comply and will comply with PCI DSS. However, PayPal's compliance, and your Product's, are not sufficient to achieve compliance with PCI DSS by you and your systems and processes.

4.4. 3D Secure

Requirements of the European Central Bank and PayPal's bank regulators require use of 3D Secure in certain circumstances, and Card Associations may also require it to reduce an excessive number of Card Transactions unauthorised by the cardholder. PayPal may by notice to you require that you implement 3D Secure for all or certain specified Card Transactions. You agree to implement 3D Secure if required in such a notice, where the issuer of a particular card supports 3D Secure for that card.

4.5. Price and currency

You may not submit payment transactions in which the amount is the result of dynamic currency conversion. This means that you may not list an item in one currency and then accept payment in a different currency. If you are accepting payments in more than one currency, you must separately list the price for each currency.

4.6. Compliance with Data Protection Addendum

You (as a "Merchant") and we agree to comply with the data protection addendum found here, which forms part of this Agreement. The terms of the data protection addendum prevail over any conflicting terms in this Agreement relating to data protection and privacy.

4.7. Data Portability

Upon any termination or expiry of this Agreement, PayPal agrees, upon written request from Merchant, to provide Merchant's new acquiring bank or payment service provider ("Data Recipient") with any available credit card information including personal data relating to Merchant's Customers ("Card Information"). In order to do so, Merchant must provide PayPal with all requested information including proof that the Data Recipient is in compliance with the Association PCI-DSS Requirements and is level 1 PCI compliant. PayPal agrees to transfer the Card Information to the Data Recipient so long as the following applies: (a) Merchant provides PayPal with proof that the Data Recipient is in compliance with the Association PCI-DSS Requirements (Level 1 PCI compliant) by providing PayPal a certificate or report on compliance with the Association PCI-DSS Requirements from a qualified provider and any other information reasonably requested by PayPal; (b) the transfer of such Card Information is compliant with the latest version of the Association PCI-DSS Requirements; and (c) the transfer of such Card Information is allowed under the applicable Association Rules, and any applicable laws, rules or regulations (including data protection laws).

5. How our other legal documents apply

5.1. Legal Agreements

You can find this Agreement, the User Agreement, the Commercial Entity Agreements and the Privacy Statement on the Legal Agreements page by clicking the Legal link at the bottom of a PayPal web page.

5.2. User Agreement

The User Agreement forms part of this Agreement. As much as possible, this Agreement and the User Agreement should be interpreted as a consistent whole. Where a conflict of interpretation arises, this Agreement overrides the User Agreement to the extent of the conflict, except in relation to your use of any of the Products or individual Online Card Payment Services as part of our PayPal Complete Payments product as set out in the User Agreement.

Capitalised words which are not defined in this Agreement are defined in that User Agreement. The definition of "Services" and "Agreement" in the User Agreement, when read together with these terms, includes the **Products and this Agreement**.

The User Agreement includes important provisions which:

5.2.1. Permit PayPal to take a Reserve to secure your obligation to pay Chargebacks, Reversals and fees;

5.2.2. Obligate you to follow PayPal's Acceptable Use Policy in your use of PayPal;

5.2.3. Give legal effect to PayPal's Privacy Statement, which governs our use and disclosure of your information and that of Shared Customers; and

5.2.4. Permit PayPal to restrict a payment or your PayPal Account in circumstances listed in the User Agreement.

You are responsible for Chargebacks, Reversals and other invalidated payments as provided in the User Agreement, regardless of how you use and configure your Product, including its fraud filtering technology and similar preventive tools (if any). Those tools can be useful in detecting fraud and avoiding payment failures, but they do not affect your responsibility and liability pursuant to the User Agreement for Chargebacks, Reversals and payments which are otherwise invalidated.

5.3. Commercial Entity Agreement

By agreeing to be bound by this Agreement, you also agree to the **Commercial Entity Agreements**. These are your direct agreements with the Acquiring Institutions, PayPal's banking partners, who enable you to receive card payments and card-funded PayPal payments.

5.4. Privacy Statement

You confirm that you have read, consented and agreed to PayPal's Privacy Statement, which explains the information that we collect about you and your online business. In particular, you agree and consent that PayPal may obtain from a third party your credit history and financial information about your ability to perform your obligations under this Agreement; the PayPal Privacy Statement lists the companies involved in this exchange of credit-related information. PayPal will review your credit and other risk factors of your Account (reversals and chargebacks, customer complaints, claims etc.) on an ongoing basis, and we may also review your website and the products for sale on it. PayPal will store, use and disclose all information that we have about you in conformity with PayPal's Privacy Statement.

5.5. Additional terms for American Express card acceptance

If we allow you to receive payments from American Express cards, this section 5.5 applies to you.

5.5.1. Commercial Marketing Communications

American Express may use the information obtained in your application at the time of setup to screen and/or monitor you in connection with card marketing and administrative purposes. By accepting these terms, you agree to receive commercial marketing communication from American Express. You may opt out by notice by contacting us. Visit our PayPal Help Centre page accessible from your User Agreement and most PayPal web pages to find out how to contact us. If you opt out of commercial marketing communications, you will still receive important transactional or relationship messages from American Express.

5.5.2. Direct Card Acceptance

You acknowledge that if you reach certain monthly and/or annual sales volumes relating to American Express as set by American Express for the time being and from time to time, American Express may require you to enter into a direct contractual relationship with them. In this situation, American Express will set pricing for American Express transactions, and you will pay fees for American Express transactions directly to American Express.

5.5.3. Audit Rights

American Express may conduct an audit of you at any time, for the purpose of determining compliance with the American Express Rules.

5.5.4. Submission and Settlement Rights

You authorise PayPal to submit transactions to, and receive settlement from, American Express, and to disclose transaction and merchant information to American Express to perform analytics and create reports, and for any other lawful business purposes,

including commercial marketing communications purposes and important transactional or relationship communications. Merchant may terminate its acceptance of American Express at any time upon notice.

5.5.5. Third Party Beneficiary

American Express shall be a third-party beneficiary of this Agreement for purposes of American Express card acceptance. As a third-party beneficiary, American Express shall have the right to enforce directly against you the terms of this Agreement as related to American Express Card acceptance. You acknowledge and agree that American Express shall have no responsibility of liability with regard to PayPal's obligations to you under this Agreement.

5.5.6. Card Present, Unattended Terminals and Payment Kiosks

You shall not accept American Express cards for any payment under this Agreement when the card is either (i) presented at a physical point of the purchase or transaction; (ii) used at unattended establishments (e.g., customer activated terminals) or (iii) presented at a payment kiosk. In addition, you shall be prohibited from providing or making available to any American Express cardmember that comes to its physical location, a computer or an online interface that will enable the American Express cardmember to access their PayPal Account.

6. Intellectual property and ID codes

6.1. Licence

PayPal hereby grants to you a non-exclusive, non-transferable, revocable, non-sublicenseable, limited license to (a) use your Product in accordance with the documentation provided on the PayPal Website; and to (b) use the documentation provided by PayPal for your Product and reproduce it for internal use only within your business. Your Product as licensed is subject to change and will evolve along with the rest of the PayPal system; see section 9.1. You must comply with the implementation and use requirements contained in all PayPal documentation and instructions accompanying the Product issued by PayPal from time to time (including, without limitation, any implementation and use requirements we impose on you to comply with applicable laws and card scheme rules and regulations).

6.2. ID codes

PayPal will provide you with certain identifying codes specific to you. The codes identify you and authenticate your messages and instructions to us, including operational instructions to PayPal software interfaces. Use of the codes may be necessary for the PayPal system to process instructions from you (or your website). You must keep the

codes safe and protect them from disclosure to parties whom you have not authorised to act on your behalf in dealing with PayPal. You agree to follow reasonable safeguards advised by PayPal from time to time in order to protect the security of those identifying codes. If you fail to protect the security of the codes as advised, you must notify PayPal as soon as possible, so that PayPal can cancel and re-issue the codes. PayPal may also cancel and re-issue the codes if it has reason to believe that their security has been compromised, and after notifying you whenever notice can reasonably be given.

6.3. Ownership of PayPal Website Payments Pro and Advanced Credit and Debit Card Payments information and materials

As part of your access to, and use of PayPal Website Payments Pro and/or Advanced Credit and Debit Card Payments, you will be provided with certain information and materials (the "Pro Materials") for your use with the Products. All intellectual property rights associated with the Pro Materials remain the property of PayPal or the relevant Acquiring Institution (as the case may be). You agree to not give, transfer, assign, novate, sell, resell (either partly or in whole) the Pro Materials to any person.

6.4. PayPal Hosted Integrations and your intellectual property

You hereby grant to PayPal a royalty-free, worldwide non-exclusive licence to use your or any of your affiliates' names, images, logos, trademarks, service marks, and/or trade names as you may provide to PayPal when using the Products ("**Your Marks**") for the sole purpose of enabling your use of the Products (including, without limitation, the customisation of your hosted Product). Title to and ownership of Your Marks and all goodwill arising from any use hereunder will remain with you. You represent and warrant that you have the authority to grant PayPal the right to use Your Marks and you shall indemnify PayPal and keep PayPal fully indemnified on a continuing basis from any claims or losses suffered by it arising from the use of Your Marks in connection with the Products.

7. Terms of use for specific functionalities

7.1. Fraud Protection

The terms in Schedule 2 apply to your use of Fraud Protection.

7.2. Vaulting Tool

If you use the Vaulting Tool, before collecting your customers' Card Data, you will:

7.2.1. notify your customers that:

7.2.1.1. the information collected will be saved and retrievable by you for future payments from the customer including, potentially, "buyer not present" payments;

7.2.1.2. the customer can update the information; and

7.2.1.3. the customer can revoke the consent.

7.2.2. obtain your customers' consent to collect and use that information on the above basis;

7.2.3. ensure that when your customers give the above consent and opt into the feature they do so by taking a deliberate and recorded action, e.g. clicking an optional button, or checking a default-unchecked box.

7.3. Account Updater Service

7.3.1 Description. Subject to the terms of this section 7.3, PayPal may make the Account Updater Service available to you, for which PayPal will send the applicable Card Data of eligible Cards to one or more third party sources, and use information available to PayPal, to check and update the applicable Card Data. Following these checks, the applicable updated Card Data relating to your customers, if any, is processed and stored by PayPal at your direction and on your behalf to enable you to accept Recurring Billing, Recurring Payments, or other eligible transactions using the Products from its customers with the applicable updated Card Data. If the Account Updater Service is made available to you, PayPal will either provide you with email notification that the Account Updater Service has been activated on your account(s) or allow you to enable the Account Updater Service on your account(s) through your PayPal account settings. You may elect to discontinue use of the Account Updater Service at any time by providing written notice to PayPal of such election or by such other means as may be designated by PayPal.

7.3.2 Permitted Use. You acknowledge and agree that the Account Updater Service is provided solely for the purpose of updating applicable Card Data to enable your acceptance of transactions using the Products. You shall not use the Account Updater Service for any other purpose, including, without limitation, the use of any portion of the Account Updater Service data in connection with the development of any other service or product.

7.3.3 Your Obligations. You shall fully comply with applicable law and the card scheme rules in connection with its use of the Account Updater Service. Further, you shall provide your customers, whose Card(s) is/are eligible for the Account Updater Service, with all disclosures required under applicable law to enable you to use the Account Updater Service to update the customer’s Card(s). The foregoing shall include, but shall not be limited to, incorporating promptly into your standard terms and conditions, privacy policy, and/or other customer facing documentation, any language required by applicable law or the card scheme rules. You shall also provide adequate disclosures to make clear

to customers that if they do not want their applicable Card Data updated, they may request you to remove their Card that is being stored by PayPal and/or terminate their Recurring Billing or Recurring Payments agreement with you.

7.3.4 Confidentiality. You agree that you shall keep all information and Card Data provided through the Account Updater Service, if any, strictly confidential. You may not disclose any such information or Card Data to any third party and you may not use such information or Card Data for any purpose other than as may be expressly permitted.

7.3.5 Indemnification. You shall indemnify PayPal against any loss arising as a result of a breach by you of your obligations under this Section for use of the Account Updater Service.

7.3.6 Accuracy of Information. You acknowledge that the Account Updater Service may only be accurate to the extent a card issuing bank and a customer participate, and that many card issuing banks and customers may not participate. You acknowledge and agrees that the Account Updater Service may rely upon information, Card Data, and services provided to PayPal by third parties.

7.3.7 Termination. PayPal may terminate the Account Updater Service at any time upon email notice to you.

8. Termination and suspension

8.1. By you

You may terminate this Agreement by giving 30 days' prior notice to PayPal Customer Service of your intent to either:

8.1.1. terminate this Agreement only. PayPal Customer Service will confirm termination via email. This option lets you stop using your Products and paying for them, but your PayPal Account remains open and its User Agreement remains in effect; or

8.1.2. close the PayPal Account that you use with your Products (see the User Agreement for more information). This option terminates this Agreement, letting you stop using your Products and paying for them, and initiates the closure process for your PayPal Account. Your PayPal Account remains open and its User Agreement remains in effect until the closure of the PayPal Account takes effect, subject further to the provisions relating to closing your PayPal Account in the User Agreement.

If you use Advanced Credit and Debit Card Payments only, you may give PayPal Customer Service immediate notice to terminate this Agreement or close the PayPal Account that you use with Advanced Credit and Debit Card Payments as outlined in sections 8.1.1. and 8.1.2. above.

You may stop using Advanced Credit and Debit Card Payments at any time by giving prior notice to PayPal Customer Service of your intent to stop using Advanced Credit and Debit Card Payments only. PayPal Customer Service will confirm the stoppage for you via email. This option lets you stop using Advanced Credit and Debit Card Payments and paying for any future transactions, but your PayPal Account remains open and this Agreement and the User Agreement remain in effect. You may start using Advanced Credit and Debit Card Payments again at any time subject to the terms of this Agreement as amended.

You may stop your acceptance of American Express card payments using the Products at any time by giving prior notice to PayPal Customer Service.

Visit our PayPal Help Centre page accessible from your User Agreement and most PayPal web pages to find out how to contact us so that you can take the above actions.

8.2. By PayPal

PayPal may terminate this Agreement or any Product-specific part of it by doing any of the following:

a. Giving you 2 months' prior notice by email to you at your registered email address associated with your Account of PayPal's intent to terminate this Agreement or the Product-specific part of it. Unless otherwise notified, terminating this Agreement does not affect your User Agreement and your PayPal Account remains open.

b. Terminating the User Agreement that applies to the PayPal Account used with your Product. Your PayPal Account remains open and its User Agreement remains in effect until the closure of the PayPal Account takes effect, subject further to the provisions relating to closing your PayPal Account in the User Agreement.

8.3. By events

PayPal may terminate this Agreement immediately without notice if you:

8.3.1. Breach this Agreement or the User Agreement;

8.3.2. Become unable to pay or perform your obligations as they fall due;

8.3.3. Become unable to pay your debts (within the meaning of section 123 of the Insolvency Act 1986), admit your inability to pay your debts or otherwise become insolvent;

8.3.4. Have any distraint, execution, attachment or similar action taken, levied or enforced against you or your assets, or if any garnishee order is issued or served on you;

8.3.5. Become the subject of any petition presented, order made or resolution passed for the liquidation, administration, bankruptcy or dissolution of all or a substantial part of your business, except where solvent amalgamation or reorganisation is proposed on terms previously approved by PayPal,

8.3.6. Lose full and unrestricted control over all or part of your assets because of the appointment of a receiver, manager, trustee, liquidator or similar officer;

8.3.7. Enter into or proposes any composition or arrangement concerning your debts with your creditors (or any class of its creditors);

8.3.8. A material adverse change occurs in your business, operations, or financial condition; or

8.3.9. You provide inaccurate information in applying for your Product or in your dealings with us.

8.4. Effect of termination

When this Agreement or any part of it terminates, you must immediately stop using the terminated Products, and PayPal may prevent or hinder you from using them after termination. If you nevertheless use a Product after termination of this Agreement, then this Agreement will continue to apply to your use of that Product until you give effect to the termination by stopping your use of that Product. The following sections in this Agreement shall survive termination of this agreement and continue in full force and effect: sections 2., 4.1., 8.2., 8.4. Termination of this Agreement or any part of it shall not affect any rights, remedies or obligations of the parties that have accrued or become due prior to termination, and you will not be entitled to a refund of any Monthly Fee applicable to any period prior to termination.

8.5. Breach and suspension

If you breach this Agreement, the User Agreement, or a security requirement imposed by PCI DSS, PayPal may immediately suspend your use of your Product (in other words, we may render your Product temporarily inoperable). PayPal may require you to take specified corrective actions to cure the breach and have the suspension lifted, although nothing in this Agreement precludes PayPal from pursuing any other remedies it may have for breach. In addition, if PayPal reasonably suspects that you may be in breach of this Agreement or PCI DSS, PayPal may suspend your use of your Product pending further investigation.

If PayPal suspends your access to or use of PayPal Website Payments Pro or Advanced Credit and Debit Card Payments, PayPal will notify you and explain the basis of PayPal's actions in suspending your use of your Product, and may specify corrective actions to cure the breach and have the suspension lifted. PayPal's suspension of your access or use of PayPal Website Payments Pro or Advanced Credit and Debit Card Payments will

remain in effect and until such time as PayPal is satisfied that you have remedied the applicable breach(es).

9. Miscellaneous

9.1. Future of the Products

PayPal retains sole and absolute discretion in determining (a) the future course and development of the Products, (b) which improvements to make in them and when, and (c) whether and when defects are to be corrected and new features introduced. PayPal welcomes feedback from users in planning the future of the Products but is not required to act in accordance with any feedback received. In giving us feedback, you agree to claim no intellectual property interest in your feedback.

9.2. No warranty

Your Product and all accompanying documentation are provided to you on an “as is” basis.

PayPal does not give or offer any warranty, express or implied, by operation of law or otherwise, in relation to:

- your Product;
- the licensed software; and
- user documentation provided.

Nothing provided by PayPal under this Agreement or otherwise for your Product has PayPal’s authorisation to include a warranty.

No obligation or liability will arise out of PayPal’s rendering of:

- technical advice;
- programming advice; or
- other advice or service,

in connection with any Product, licensed software and user document provided. This includes, among other matters, services that may assist you with the customisation of your Product.

PayPal recommends that you test the implementation of your Product thoroughly as PayPal is not responsible for any loss caused by a defect in it.

If PayPal hosts your Product (in other words, we run the software for you as a web service), PayPal does not guarantee continuous, uninterrupted or secure access to your hosted Product.

PayPal will not be liable for any delay or failure in hosting your Product.

You acknowledge the availability of your Product for use may be occasionally limited to allow for repairs, maintenance or the introduction of new facilities or services.

Some countries do not allow the disclaimer of implied warranties, so the foregoing disclaimers might not apply to you.

9.3. Indemnity

You agree to indemnify PayPal and keep PayPal fully indemnified on a continuing basis from any direct loss, damage and liability, and from any claim, demand or cost (including reasonable attorneys' fees) incurred in relation to any third party (including a Shared Customer) and arising out of your breach of this Agreement, the User Agreement and the documents incorporated in it by reference (including the Acceptable Use Policy), or the violation of any law.

9.4. Assignment, amendment and waiver

You may not assign this Agreement without first obtaining PayPal's written consent. PayPal may assign, novate or otherwise transfer this agreement without your consent by notifying you. Neither party may amend this Agreement or waive any rights under it except in a written document signed by both parties.

9.5. English law and jurisdiction

This Agreement is governed by the laws of England and Wales. You and we submit to the non-exclusive jurisdiction of the courts of England and Wales.

10. Definitions

Capitalised terms not listed in this section are defined in the User Agreement.

"**3D Secure**" means a security procedure that enables a card-issuing bank to authenticate the cardholder authorising a Card Transaction at the time a payment is made. 3D Secure has other brand names depending on the Card Association whose branding appears on the card; brand names for 3D Secure include Verified by Visa and MasterCard SecureCode.

"**Account Updater Service**" means a functionality as further defined in section 7.3.

"**Acquiring Institution**" means a financial institution or bank that provides services to you and PayPal to enable you to (a) accept payment by cardholders using cards: and (b) receive value in respect of Card Transactions.

"**Activation Date**" means the date on which you complete all of the steps for "Getting started" as listed in section 1 above.

"**Advanced Credit and Debit Card Payments**" means a Product as further defined in the About your Agreement section.

"**Advanced Credit and Debit Card Payments API**" means an Online Card Payment Service as further defined in the About your Agreement section.

"**Advanced Fraud Management Filters**" means a technology provided by PayPal to enable you to (a) check a card payment against criteria such as the cardholder's billing address (Address Verification Service or AVS), the card's CVV2 Data, and databases of suspicious addresses, identifiers, and patterns. See the PayPal Website and product documentation for further information. Advanced Fraud Management Filters offer a greater level of transaction screening, and transactions can be automatically flagged, reviewed or declined based on how you configure the filters.

"**AVS Data**" means information returned by the Address Verification System operated by or on behalf of Card Associations, which compares address data provided by an apparent cardholder with address data on file for the card at the card issuer.

"**Card Association**" means a company or consortium of financial institutions which promulgates rules to govern Card Transactions that involve the card that carries the company's or the consortium's brand. Examples include Visa USA, Visa Europe, and the other Visa regions; Mastercard International Incorporated; American Express Company and similar organisations.

"**Card Data**" means all personal or financial information relevant to a Card Transaction, including information recorded on the card itself (whether in human-readable form or digitally), together with the cardholder's name and address and any other information necessary for processing a Card Transaction.

"**Card Transaction**" means a payment made using a credit or debit card, an American Express card, or any other payment method using a physical data-carrying item intended to be held in the payer's possession. The Products support only certain types of Card Transactions; see the PayPal Website for more information.

"**Critical Systems**" means the information technology (both hardware and software) that you employ to operate your Products, to protect them and your online points of sale against intrusion and interference, and to store payment-related and personal data, including any Card Data that you retain and all personal data about Shared Customers.

"**CVV2 Data**" means the three-digit number printed to the right of the card number in the signature panel area on the back of the card. (For American Express cards, the code is a four-digit unembossed number printed above the card number on the front of the American Express card.) The CVV2 Data are uniquely associated with each individual plastic card and ties the card account number to the plastic.

"**Data Breach**" means an intrusion into or malfunction of a computer system in which Card Data are stored, and which intrusion or malfunction either (a) exposes, modifies or destroys all or part of the Card Data in the system, or (b) runs a significant risk, in the opinion of a qualified expert in information security, of exposing, modifying or destroying all or part of the Card Data in the system. Card Data are exposed where they are released from the normal access controls of the system without authorisation, or where they are actually disclosed to one or more unauthorised persons.

"**Direct Payments API**" means an Online Card Payment Service as further defined in the About your Agreement section.

"**Express Checkout**" means a Functionality for expediting online retail checkout by using information provided to you by PayPal. Details about Express Checkout appear on the **PayPal Website** and in the documentation that PayPal provides for PayPal Website Payments Pro and Advanced Credit and Debit Card Payments.

"**Fraud Protection**" means a technology provided by PayPal to enable you to (a) check a card payment against criteria such as the cardholder's billing address (Address Verification Service or AVS), the card's CVV2 Data, and databases of suspicious addresses, identifiers, and patterns, offered together with the Advanced Credit and Debit Card Payments API as an alternative to the Advanced Fraud Management Filters.

"**General Data Protection Regulation**" means the Regulation (EU) 2016/679 (General Data Protection Regulation)or any successor to it, together with all other laws about the privacy of citizens or residents of the member state of the European Economic Area in which you reside or are established as a business enterprise.

"**Hosting Option**" means any of the following: (i) a PayPal Hosted Integration; or (ii) a Self Hosted Integration.

"**Monthly Fee**" means a fee payable on a monthly basis as required in section 2 above.

"**Online Card Payment Services**" means a functionality provided online by PayPal to enable merchants to receive payments directly from a payer's card (without the funds passing via the payer's PayPal Account), without the card being present at the website or other point of sale. Online Card Payment Services are integral to the Products The Online Card Payment Services are listed and further defined in the About your Agreement section.

"**PayPal Hosted Integration**" means PayPal's Direct Payments API or Advanced Credit and Debit Card Payments API integrated into the payment process of your website pursuant to section 1, with that functionality being operated (including the card entry field being hosted) entirely on PayPal's server (rather than on your website).

"**PayPal Website**" means the website provided by PayPal for the country in which you reside. In the case of the UK, the PayPal Website is currently at http://www.paypal.co.uk. References to PayPal Websites for other countries can be found via a link from any other PayPal Website.

"**PCI DSS**" means the Payment Card Industry Data Security Standard, which consists of specifications prescribed by Card Associations to ensure the data security of Card Transactions. A copy of PCI DSS is available online from **https://www.pcisecuritystandards.org/**.

"**Product**" or "**Your Product**" means whichever one of the Products you access and use after accepting this Agreement. The Products are listed and further defined in the About your Agreement section.

"**Qualified Security Assessor**" has the meaning given it in PCI DSS.

"**Recurring Payments Tool**" means a technology provided by PayPal for setting up payments that recur at specified intervals or frequencies with authorisation from the payer. See the PayPal Website and product documentation for further information.

"**Self Hosted Integration**" means PayPal's Direct Payments API or Advanced Credit and Debit Card Payments API integrated into the payment process of your website pursuant to section 1, with that functionality being operated (including the card entry field being hosted) at least in part on your website.

"**Shared Customer**" means a person who has a PayPal Account and is also your customer.

"**Standard PayPal Payments**" means all Payments which you receive from another PayPal account or payments via PayPal's Account Optional Service or from Local Payment Methods.

"**User Agreement**" means the contract entered into online as part of the online registration process required to open a PayPal Account. The current User Agreement is to be found via a link from the footer of nearly every page on the PayPal Website. It includes certain policies, notably the Acceptable Use Policy, which are also listed on the PayPal Website.

"**Vaulting Tool**" means an API-based technology provided by PayPal to enable you to store and retrieve card details for payments that recur at specified intervals or frequencies

with authorisation from the payer. See the PayPal Website and product documentation for further information.

"**Virtual Terminal**" means a functionality provided by PayPal to enable you to receive a card payment by manually entering Card Data given you by the cardholder. Virtual Terminal is one of the Online Card Payment Services and also a standalone Product as further defined in the About Your Agreement section.

"**Website Payments Pro**" means a Product as further defined in the About your Agreement section.

Schedule 1

Data Security Requirements

Website Payment Pro, Advanced Credit and Debit Card Payments and Virtual Terminal enable you to accept payments online directly from debit and credit cards, which are payment instruments whose security depends on controlling the disclosure of Card Data. A person who has sufficient Card Data can send or receive a card payment charged to the cardholder's account without necessarily having the cardholder's authorisation for the payment. To prevent your Shared Customers from having their Card Data misused, you must keep Card Data secret at all times. The General Data Protection Regulation also requires you to keep a Shared Customer's personal data secure.

PayPal strongly recommends that you obtain the services of a competent professional expert in information security to advise you and assist in securing your website and any other points of sale.

Principles of Data Security

1. **Design and development**

You must design and develop your Critical Systems and all payment-related processes so that they are secure from intrusion and interference by unauthorised persons. All users of your systems must be required to authenticate themselves to your Critical Systems, and those Systems must limit the access and powers of their users. You must also organise your business so as to segregate critical duties and create controls and checkpoints in your operations, rather than place too much unchecked power over your systems and operations in one person. Never give a user more power over your systems and processes than the minimum necessary for the user to perform his or her assigned role.

2. **Protection against intrusion**

You must divide your operations into two basic categories, (1) those functions available to all users including those outside your organisation, and (2) those available only to trusted people within your organisation. You must employ a firewall to block untrusted users from the using internal-only functions of your Critical Systems. Your web servers and other external-facing portions of your Critical Systems must use well developed and thoroughly tested technology, and make available externally only those functions which are necessary for Shared Customers and other external users to use. Strip your external-facing servers of all superfluous functions to protect (harden) them and reduce their vulnerability to external attack.

3. **Access controls**

Your Critical Systems must restrict access to Card Data and all other personal or important data to only trusted persons within your organisation, and no such person should have greater access to such data than is necessary for that person to perform his or her role. Your systems must track and log all access, use, modification and deletion of Card Data and other personal or important data so that you maintain an audit trail of all such actions. You must also limit access to your Critical Systems and the resources on which they depend such as networks, firewalls, and databases.

4. **Data minimization**

As a general principle, you should gather and retain no more Card Data or other sensitive data than you need. Holding Card Data and personal data creates a risk of liability to you, and you can reduce that risk by taking and holding less data. If you store Card Data, consider carefully the need to do so: PayPal must refund a payment which lacks its payer's authorisation, and if the user will authorise a further payment, the user will generally also give you up-to-date Card Data again, so you may have little need to store Card Data for future use. Card Data that you do not have is data that you cannot spill if you suffer a Data Breach.

5. **Changes and testing**

Except in emergencies, avoid changing Critical Systems without first planning, testing, and documenting the change, unless the change is routine (*e.g.* adding a user, changing a password, updating inventory and prices). For major systemic changes or those which can impact the security or availability of your Critical Systems, planned changes should be escalated for approval by high-ranking managers other than the planners of those changes. Implement planned changes in your production systems only after they have been thoroughly tested in a non production environment. Conduct all such testing under the supervision of the your risk management department or others in your company with particular responsibility for its losses.

6. **Audits**

You must audit the operations and security of your Critical Systems at least once a year. This systems audit must be distinct from any audit of your finances. Use trusted and independent experts to audit your Critical Systems, and if you use your employees as auditors, ensure their independence by protecting their employment from retaliation and by isolating them from the work of administering, operating, changing and testing your Critical Systems.

7. **Outsourcing and organisational control**

You must ensure that all persons who have access to your Critical Systems, or who design, develop, operate, maintain, change, test and audit your Critical Systems comply with this Agreement and PCI DSS. You are responsible to ensure compliance even if such persons are not your employees.

What to do in case of a Data Breach

8. **Data Breach**

If you experience a Data Breach, you agree to do all of the following:

a. Take whatever action you can to stop the Data Breach and mitigate its consequences immediately after discovering the Data Breach.

b. Notify PayPal as soon as possible after discovering the Data Breach by contacting your account manager (if one is assigned to you) or contacting our Customer Service (details of how to contact us are on the **"Contact Us"** page). If you cannot simultaneously do (a) and notify PayPal, then do (a) first and then notify PayPal.

c. Notify all Shared Customers whose Card Data has been exposed or which is likely to have been exposed, so that those Shared Customers can take steps to prevent misuse of the Card Data. You further agree to complete this notification immediately after you perform (a) and (b) above, to notify PayPal when you have completed this notification, and to provide a list of Shared Customers whom you have notified. If you fail to complete this step promptly after the Data Breach, PayPal may notify Shared Customers of the Data Breach, and will identify the Shared Customers from your PayPal Account records of who has paid you using a card.

d. If requested by PayPal, have an independent third party auditor, approved by PayPal, conduct a security audit of your Critical Systems and issue a report. You agree to comply with PayPal's request under this section at your own expense. You must provide a copy of the auditor's report to PayPal, and PayPal may provide copies of it to the banks (including, without limitation, Acquiring Institutions) and Card Associations involved in processing card transactions for PayPal. If you do not initiate a security audit with 10 business days of PayPal's request, PayPal may conduct or obtain such an audit at your expense. See also Schedule 1 on Audit.

e. Cooperate with PayPal and follow all reasonable instructions from PayPal to avoid or mitigate consequences of the Data Breach, to improve your Critical Systems so that they satisfy the requirements this Agreement, and to help prevent future Data Breaches. However, PayPal shall not require you to do more than this Agreement requires, unless the additional measures are reasonable in light of the risk to Shared Customers and the best practices of online retailing.

f. Resume normal operation of your Critical Systems only when you have ascertained how the Data Breach occurred and taken all reasonable steps to eliminate the vulnerabilities that made the Data Breach possible or which could make other Data Breaches possible;

g. Report the Data Breach to law enforcement authorities, cooperate in any investigation that they undertake, and cooperate as the authorities may request in order to identify and apprehend the perpetrator of the Data Breach.

h. Refrain from using Card Data that have been exposed or modified in the Data Breach. However, this section does not prevent you from obtaining and using Card Data again from Shared Customers affected by the Data Breach, after the vulnerabilities in your Critical Systems have been remedied pursuant to (f) above.

Data protection

9. **See Section 4 for Data Protection terms.**

10. **Intentionally left blank.**

Card Data and PCI DSS

11. **Retention of Card Data**

Unless you receive and record the express consent of the cardholder, you may not retain, track, monitor or store any Card Data. You must completely and securely destroy all Card Data that you retain or hold within 24 hours after you receive an authorisation decision from the issuer relevant to that Card Data.

> If, with the cardholder's consent, you briefly retain Card Data, you may do so only to the extent that the Card Data are necessary for processing payment transactions with the cardholder's authorisation. You must never give or disclose the retained Card Data to anyone, not even as part of the sale of your business. Moreover, and regardless of anything to the contrary, you must never retain or disclose the card verification and identification data printed in the signature stripe on the back of the card (i.e. the CVV2 Data), not even with the cardholder's consent.

12. **Card Data that you must not store**

Notwithstanding the immediately preceding section, you agree to not store any personal identification number (PIN) data, AVS Data, CVV2 Data, or data obtained from the magnetic stripe or other digital storage facility on the card (unless that data is also printed or embossed on the front of the card) of any cardholder. Card associations may impose fines if you violate this section, which reflects card association rules. In this section, 'store' means retain in any form, whether digital, electronic, paper-based, or otherwise, but does not include temporary capture and holding of data while it is actively being processed (but not afterwards).

13. **Merchant's use of Card Data**

You agree not to use or disclose Card Data except for the purposes of obtaining authorisation from the card issuer, completing and settling the Card Transaction for which the Card Data was given to you, together with resolving any Chargeback or Reversal Dispute, or similar issues involving Card Transactions. PayPal is required by banking laws to refund payments lacking the payer's authorisation, so your use of Card Data to carry out a Card Transaction must be authorised by the cardholder or it will subject to Reversal.

14. **Secure storage and disposal of Card Data**

You agree to:

a. establish and maintain sufficient controls for limiting access to all records containing Card Data;

b. not sell or disclose to a third party any Card Data or any information obtained in connection with a Card Transaction;

c. keep no Card Data on paper or in portable digital storage devices such as USB memory devices or removable disks;

d. not reproduce any electronically captured signature of a cardholder except on PayPal's specific request; and

e. destroy Card Data either by destroying the medium on which the Card Data are stored or by erasing or rendering the Card Data completely and irreversibly unintelligible and meaningless.

> If you transfer your business, Card Data and any information you have about Card Transactions is not transferable under Card Association rules as an asset of the business. In such cases, you agree to provide the Card Data and any transactional data to PayPal if it requests. If PayPal does not request such data, you must destroy it when your business transfers.

15. **PCI DSS audit**

If PayPal so requests, you agree that a Qualified Security Assessor may conduct a security audit of your systems, controls and facilities and issue a report to PayPal and the Associations. You agree to cooperate fully in the conduct of this audit, and to provide any information and access to your systems required by the auditor for the performance of the audit. You also agree to bear the reasonable expenses of this audit. If you fail to initiate such an audit after PayPal requests you to do so, you authorise PayPal to take such action at the Merchant's expense, or PayPal may immediately suspend your use of your Product. You will receive a copy of the audit report, and PayPal must also receive a copy and provide a copy to any Acquiring Institution or Card Association that requests a copy.

Schedule 2

Terms of use of Fraud Protection ("Fraud Tool")

1. **How the Fraud Tool works**

The **Fraud Tool** is made available to you as a fraudulent transaction management tool to help you screen potentially fraudulent transactions based on the settings you adopt in the Fraud Tool. The tool allows you to set filter rules, i.e. to instruct us about which transactions the tool shall decline on your behalf based on abstract criteria.

We may provide suggestions or recommendations regarding what filters and settings in the Fraud Tool to use that may be appropriate for your business. These suggestions take into account your past transaction history.

It is your responsibility to set the filter rules. Please note: If you set these filter rules too restrictively, you might lose sales volume. We advise you to monitor your filter rules and settings on an ongoing basis.

2. **No Warranty and Limitation of Liability**

We do not represent or warrant that the Fraud Tool is error-free or that it will identify all potentially fraudulent transaction activity.

We are not liable for your losses (such as loss of profits) or damages arising from or related to your use of the Fraud Tool, to the extent that applicable law allows.

The Sections "Other Legal Terms – Indemnification and Limitation of Liability – Limitation of Liability" and "Other Legal Terms – Indemnification and Limitation of Liability – No warranty", "About your account – Closing your PayPal Account", "Other Legal Terms – Indemnification and Limitation of Liability – Release of PayPal" of the User Agreement apply.

3. **Data Protection**

You may only use the Fraud Tool for the purpose of your management of fraud risk and for no other purpose.

You may not share use of the Fraud Tool with any other person, nor may you disclose to any person the categories provided in the Fraud Tool or the results generated from your use of the Fraud Tool.

4. **Miscellaneous**

Despite your settings on the Fraud Tool, We always retain the right to decline or suspend any transaction pursuant to the terms of the User Agreement.

These terms supplement the **User** Agreement that governs your use of our services in general. The definition of our Services in the User Agreement, when read together with these terms, includes the Fraud Tool.

We may amend, delete or add to these terms in line with the Change process set out in the User Agreement. If you do not agree with any Change, you may terminate these terms.

You may terminate these terms at any time by removing the Fraud Tool from your integration and following any other integration-related steps which we may make available to you. This lets you stop using the Fraud Tool, but otherwise your Account remains open and the User Agreement (and any other relevant agreements relating to the provision of Services to you) remains in effect.

We may, at any time, for any reason and (where possible) with reasonable prior notice, terminate, cancel or suspend the Service to the extent it relates to our **Fraud Tool** without liability towards you.

These terms survive any termination to the extent and for so long as we require to: (i) deal with matters arising from your use of the Fraud Tool prior to termination; and/or (ii) comply with applicable laws and regulations.